BUNDESREPUBLIK DEUTSCHLAND

36

EP04/51749

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 36 805.1

Anmeldetag: 11. August 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: Verfahren zum Übermitteln von geschützten Informationen an mehrere Empfänger

IPC: H 04 L, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 21. September 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wallner

A 9161
03/00
EDV-L

Beschreibung

Verfahren zum Übermitteln von geschützten Informationen an mehrere Empfänger

Fachgebiet der Erfindung

Die Erfindung betrifft ein Verfahren gemäß der unabhängigen Ansprüche 1 und 2.

In den vergangenen Jahren ist es immer populärer geworden, über die verschiedenen Kommunikationsnetze Dienste in Anspruch zu nehmen oder Waren zu erwerben. Ein Hinderungsgrund war für den Benutzer bisher immer, dass auch sensible Daten, wie Kontoinformationen, über das Netz übertragen werden müssen.

In der Figur 1a ist ein Kaufvorgang vorgestellt, wie er derzeit beispielsweise im Internet durchgeführt wird. Auf der einen Seite steht der Kunde (Consumer), der bei einem Verkäufer (Merchant) Waren erwirbt. Die Bezahlung dieser Waren soll über sein Bankkonto erfolgen. Der Consumer übermittelt nun seine Warenanforderung an den Verkäufer, hier sind verschiedene Informationen denkbar, wie Zusatzinformationen (Userinfo), eine Angabe über die gewünschten Waren (Goods), sowie Information über die gewünschte Zahlunsweise, beispielsweise eine Kreditkartennummer.

Diese Informationen werden dem Verkäufer übermittelt, etwa über eine gesicherte Leitung (SSL, Secure Socket Layer, und TLS, Transport Layer Security, eine gesicherte Verbindung). Diese Verbindung kann zwar von Fremden nicht abgehört werden, jedoch erhält so auch der Verkäufer Informationen, die nicht unbedingt für ihn bestimmt oder zum Abschluß des Kaufvertrages notwendig sind, wie eben die Kreditkartennummer. Der Verkäufer leitet diese Informationen vollständig an die Bank weiter, insbesondere auch die Information über die gekauften Waren, die nicht für die Bank bestimmt sind.

Gewünscht wäre jedoch ein Verhalten, wie es in der Figur 1b dargestellt ist, so dass der Verkäufer nur die für ihn wichtigen Informationen über die bestellten Waren erhält und die Bank nur die für sie wichtigen Informationen über das Konto des Kunden.

Stand der Technik

Verschiedene Lösungen sind bereits bekannt. Ein bekanntes Produkt auf dem Gebiet der elektronischen Bezahlverfahren wird von der Firma SET Secure Electronic Transactions Llc. angeboten. Eine Beschreibung des bekannten Verfahrens findet man in der Spezifikation der Software, die auf ihrer Webseite http://www.setco.org/extensions.html abgelegt sind. Hier findet sich eine Datenstruktur, die durch zusätzliche Erweiterungen, sogenannte "extensions", anwendergerecht ergänzt werden kann.

Auch in dieser Lösung von SET wird jedoch keine Möglichkeit angegeben, verschiedene inhaltlich zusammengehörende Informationen, beispielsweise Kreditkartennummern mehrerer Anbieter oder Kontoangaben verschiedener Banken, zusammen in einer Datenstruktur abzulegen.

Aufgabe der Erfindung ist es also, ein Verfahren zum Übermitteln von Informationen anzugeben, welches es den Empfängern ermöglicht, die für sie bestimmten Teile der Informationen zu lesen. Aufgabe ist es weiterhin, mehrere inhaltlich zusammengehörige Daten in einer einzigen Datenstruktur geschützt zu übermitteln.

Diese Aufgabe wird gelöst durch ein Verfahren gemäß des Patentanspruchs 1 und durch ein Verfahren gemäß des Patentanspruchs 2.
Gemäß dem Patentanspruch 1 werden erste Informationen, die für einen ersten Empfänger, im weiteren auch Anbieter ge-

nannt, bestimmt sind, zusammen mit zweiten Informationen, welche für einen zweiten Anbieter bestimmt sind, in einer gemeinsamen Informationseinheit versendet. Die ersten Informationen können dabei gemäß den Vorgaben des ersten Anbieters verschlüsselt sein. Die zweiten Informationen, welche aus mehreren Bestandteilen bestehen können, werden gemäß den Vorgaben des zweiten Anbieters verschlüsselt, beispielsweise mit einem öffentlichen Schlüssel, einems sogenannten "public key". Diese "public key" Verschlüsselungsverfahren sind bereits in verschiedenen Ausführungen und Sicherheitsstufen bekannt. Durch dieses Vorgehen wird gewährleistet, dass der erste Anbieter bei Erhalt der kompletten Information die für ihn nicht bestimmten Informationsanteile nicht entschlüsseln kann.

Der Empfänger der Nachricht wird im weiteren auch Anbieter genannt, da in den beschriebenen Beispielen im wesentlichen auf einen Kaufvorgang im Netz eingegangen wird. Hier ist der erste Empfänger der Nachricht üblicherweise ein Verkäufer, also ein Anbieter von Waren und Dienstleistungen, der zweite Empfänger der Nachricht eine Bank oder Geldinstitut, also ein Anbieter von Finanzdienstleistungen. Diese Beschreibungen sind jedoch nicht einschränkend gemeint.
Andere Konstellationen sind vorstellbar, beispielsweise ein Anbieter von Informationen, der auf weitere Datenbanken zugreift, ein erster Netzbetreiber, der auf ein Netz in einem fremden Land zugreift, ein Automobilhersteller oder Polizei, die auf die Datenbank der Kfz-Anmeldestelle zugreifen.

Patentanspruch 2 gibt eine alternative Lösungsmöglichkeit an, bei der die Informationen, welche für den zweiten Anbieter gedacht sind, nicht mit den ersten Informationen zusammen in das Netz geschickt werden, sondern bei Bedarf von dem Informationsempfänger aus einem zentralen Speicherbereich im Netz abgeholt werden können.

Vorteilhafte Ausgestaltungen und Weiterbildungen sind in den Unteransprüchen angegeben.

Als besonders vorteilhaft hat sich eine Realisierung der erfindungsgemäßen Lösung gemäß dem bereits bekannten Standard X.509 erwiesen (Series X: Data Networks and Open Systems Communication - Directory: Public Key an Attribute that Certificate Frame Works, ITU-T Recommendation X.509). Eine Realisierung mit dem X.509-Standard birgt mehrere Vorteile in sich, denn dieses Vorgehen ist bereits standardisiert, und kann unabhängig von bereits vorhandenen Implementierungen verwendet werden. Eine Definition der Datenstrukturen erfolgt in ASN.1 Notation, welche ebenfalls seit Langem standardisiert ist und implementierungsunabhängig angewendet wird.

Besonders vorteilhaft erweist sich das erfindungsgemäße Verfahren bei den bereits angesprochenen Zahlungstransaktionen, die notwendig werden, wenn man Daten, Informationen und Waren über das Internet oder ein sonstiges Kommunikationsnetz bestellt oder bezieht und auch die Bezahlung über das Netz abwickeln möchte.

Im Rahmen der bereits bekannten Transaktionen über Netze hat es sich bewährt, einem Vorgang eine sogenannte Transaktionsnummer (TAN) zuzuweisen, welche einen Kaufvorgang im Netz eindeutig beziffern und auch nachträglich zurückverfolgen lassen.

Die Realisierung der Information durch Ablage in einer Erweiterung eines Zertifikats gemäß dem Standard X.509 kann in zwei verschiedenen Variationen erfolgen.

Man kann dieses Zertifikat als sogenanntes Identity Certificate realisieren, dieses ist beschrieben im ITU Standard X.509, Section 2. Vorteilhaft ist bei dieser Ausführung, dass das Zertifikat sehr kompakt wird, man hat eine "all in one"-Lösung.

Ein Zertifikat in dieser Form ist allerdings im Nachhinein nicht mehr änderbar. Daher gibt es als Alternative die Realisierung in einem sogennannte "Attribute Certificate". Die Beschreibung hierzu findet sich in der Section 3 des bereits genannten Standards. Das hat den Vorteil, dass die einzelnen Erweiterungen (Extensions) dieses Zertifikats unabhängig voneinander sind, deshalb kann man sie jederzeit ändern. Ein Zertifikat muss auch nicht widerrufen werden, man muss nur abwarten, bis seine Lebensdauer abgelaufen ist. In diesem Fall wird das System allerdings komplexer. Der Benutzer muss verschiedene Zertifikate behandeln und der Ausgebende der Zertifikate muss mehr Certificate Revocation Lists (CRL) verwalten.

Wählt man zur Realisierung die zweite Lösung, die Attribute Certificate Extension, so hat man hier noch die Auswahl, ob dieses Zertifikat genau einmal verwendet werden kann, eine sogenannte "One Time Use" oder als sogenannte "Long Life Use" einen bestimmten Zeitraum vorgibt, in dem das Zertifikat gültig ist.

Zur Ablage des Zertifikats und dazugehörige privaten Schlüssel ist ein geeignetes Speichermedium denkbar, auch wenn das Zertifikat zentral im Netz abgelegt wird. Der Eigentümer des Zertifikats kann dieses auch auf eine Smart Card oder einen Smart Dongle, auf einem kontaktlos abzulesendem Speichermedium oder ähnlichem speichern. Hierbei ist es besonders vorteilhaft, wenn das abgelegte Zertifikat zusätzlich durch ein Passwort, eine PIN usw. vor unberechtigtem Zugriff geschützt wird.

Das beschriebene Verfahren kann selbstverständlich für alle Nutzerinformationen verwendet werden, neben der Kreditkartennummer, wie Adresse, Blutgruppe, Versicherungsnummern etc..

Das vorgeschlagene Vorgehen hat gegenüber dem bereits bekannten Verfahren verschiedene Vorteile.

Eine Verschlüsselung und Signierung der Informationen mit bereits bekannten Verfahren ist jederzeit möglich. Dadurch wird der Schutz vor unberechtigtem Zugriff (die Privacy) der Informationen gesichert.

Der Diebstahl von Kreditkartennummern, wie es bisher beispielsweise durch Abhören der Kauftransaktion geschah, wird weiter erschwert. Durch eine zusätzliche Sperre des Zugriffs auf gespeicherte Informationen auf dem Speichermedium durch Einführung einer PIN wird der Schutz weiter erhöht.

Kurzbeschreibung der Zeichnungen

Im Folgenden wird die Erfindung anhand von Ausführungsbeispielen erläutert. Dabei zeigen

Figur 1a eine Übersicht über die Verbindungen, die derzeit bei einem Kaufvorgang aufgebaut werden, wenn der Käufer die Bezahlung über einen Zahlungsdienstanbieter im Netz vornimmt,

Figur 1b zeigt denselben Vorgang, wenn das erfindungsgemäße Verfahren auf den Zahlungsvorgang verwendet wird,

Figur 2a zeigt die Zertifikatserweiterungen für mehrere Kreditkarten oder ähnliche Informationen,

Figur 2b zeigt die neuen Primaten OID gemäß X.660

Figur 3a zeigt das beispielhafte Format für eine Kundenanforderung bei einem Kaufvorgang,

Figur 3b zeigt das Format für die Antwort des ersten Anbieters,

Figur 3c zeigt das Format für die signierte Erwiderung des Kunden,

Figur 3d zeigt das Format für die Authentisierungsdaten vom zweiten Anbieter, ebenfalls signiert,

Figur 3e zeigt das Format für eine zweite Kundenanforderung,

Figur 3f zeigt das Format für eine dritte Kundenanforderung,

Figur 3g zeigt das Format für eine vierte Kundenanforderung,

Figur 3h zeigt ein weiteres beispielhaftes Format für die Autorisierungsdaten vom zweiten Anbieter, ebenfalls signiert,

Figur 4 zeigt einen Kaufvorgang in vier Schritten,

Figur 5 zeigt einen Kaufvorgang in acht Schritten,

Figur 6 zeigt einen Kaufvorgang in zehn Schritten,

Figur 7 zeigt einen Kaufvorgang mit auftretenden Fehlern,

Figur 8 zeigt die Struktur des SICRYTT Secure Token,

Figur 9 zeigt die X.509 Zertifikat Extension Struktur.

Die Figuren 1a und 1b zeigen, wie in der Einleitung bereits beschrieben, den beispielhaften Ablauf eines Kaufvorganges. In den Kästen über den Pfeilen dargestellt, sind die jeweiligen Informationen, die zwischen den einzelnen Verfahrensteilnehmern fließen. Der Kontakt des Käufers (Consumer) geschieht immer über den Verkäufer (Merchant). Eine direkte Kommunikation des Käufers zur Bank findet nicht statt. Alle Informationen fließen über den Verkäufer. Dies hat zur Folge, dass der Verkäufer auch Informationen erhält, die für seinen Verkaufsvorgang unerheblich sind. Durch das erfindungsgemäße Verfahren, wie in Figur 1b dargestellt, werden dem Verkäufer zwar sämtliche Informationen übersendet, er kann diese jedoch nicht uneingeschränkt lesen. Beispielsweise die Kreditkarten-

information (Credit Card Info), wie hier durchgestrichen dargestellt, ist dem Verkäufer nicht angezeigt. Andere Informationen, etwa wir der Kunde ist (User Info) und was dieser Kunde bestellen möchte (Goods) sind ihm frei zugänglich.

Heutige Public Key Zertifikate versuchen, ein Zertifikat (Public und Private Key) auf ein vollständiges Userprofil abzubilden. Allerdings hat sich die Anzahl der Anwendungen erweitert, so dass mehr als eine Anwendung (in Zusammenhang mit beispielsweise Webdiensten) benötigt werden.
Die erfindungsgemäße Idee verwendet hierfür ein bereits bekanntes X.509 Zertifikat und erweitert dieses durch zusätzliche Informationen. Diese Informationen werden verschlüsselt und in dieser Form im Zertifikat abgespeichert. Eine Darstellung hierfür findet sich in Figur 2a.
Der ursprüngliche X.509 Standard wurde entworfen, um einen weltweit einheitliche Namen zu entwickeln für Benutzer in einem Netz, ohne doppeltes Vorkommen, in einem sogenannten X.500 Directory. Das X.500 Directory ist eine Datenbank, die für weltweiten Gebrauch bestimmt ist, wie ein weltweites Telefonbuch. Das X.509 Zertifikat wird digital signiert und durch eine Zertifizierungsautorität ausgegeben, um die Identität des Inhabers und zusätzliche Informationen zu bestätigen. Public key Verfahren sehen vor, um sicher mit anderen Telnehmer zu kommunizieren, zwei Schlüssel zu generieren: ein privaten Schlüssel (der geheim bleibt) und einen öffentlichen Schlüssel, der an jeden weiter geben werden kann. Das X.509 Zertifikat verbindet den öffentlichen Schlüssel und den Namen des Inhabers des privaten Schlüssels.
Vorteil des X.509 Standards ist es, dass er für eine allgemeine Verwendung entwickelt wurde. Hier wird das ganz allgemeine Problem der Authentisierung in verteilten Systemen gelöst und sein Lösungsentwurf ist implementierungsunabhängig.

In der Version 3 des X.509 Standards, der 1996 veröffentlich wurde, wurden sogenannte Extensions eingeführt, bei denen jedermann zusätzliche Datenfelder implementieren und diese in

seine Datenstruktur einführen kann. Diese Erweiterungen werden auch Private, Proprietary, oder Custom Extensions genannt. Sie tragen eindeutige Informationen, die für den Zertifikatinhaber oder Zertifikataussteller wichtig sind.
Bislang bekannte Erweiterungen sind heute sogenannte "Key Usage Limits", die die Verwendung eines Schlüssels auf einen speziellen Verwendungszweck beschränken, oder "Alternative Names", die der Verknüpfung des Öffentlichen Schlüssels (Public Keys) mit anderen Namen wie: Domain Namen, E-Mailadressen etc. ermöglicht. Diese Zertifikatergänzungen können auch als kritisch markiert werden um anzuzeigen, dass die Ergänzung überprüft werden muss.

Im beispielhaften Fall eines Zahlungsverkehrs teilt der Benutzer mit verschiedenen Teilnehmern verschiedene "Geheimnisse", also Daten, die nur dem direkten Kommunikationspartner bekannt gegeben werden sollen, beispielsweise bei einem Kreditkartenausgebenden, wie American Express, Visa, Master Card etc., eine Kreditkartennummer oder mit einer Bank die Kontonummer oder mit einer Versicherungsanstalt die Versicherungsnummer. Weitere persönliche Informationen, wie beispielsweise die Adresse, sind vorstellbar.
Nur der Besitzer des Zertifikats kennt alle diese Erweiterungen. Jede einzelne Erweiterung wird dann so verschlüsselt, dass nur die jeweilige Partner mit der richtigen Identität die entsprechenden Daten wieder entschlüsseln kann.

Hierfür kann beispielsweise das bekannte Public Key Kryptographie-Verfahren verwendet werden. Zur Verschlüsselung wird dann der jeweilige öffentliche Schlüssel der Versicherung, der Bank oder des Kreditkartenausgebenden verwendet. Dieses wird bei der Ausgabe des Zertifikats verwendet. Danach wird das Zertifikat in einem Public Directory abgelegt werden, weil nur der jeweilige Ausgebende der Information diese mit seinem privaten Schlüssel entschlüsseln (verstehen) kann.

Die Erweiterungen sind in dem X.509-Standard in der ASN1 Notation definiert. Die Figur 2a zeigt eine beispielhafte Ausgestaltung einer möglichen ausgegebenen Zertifikatergänzung für einen Benutzer. Dieser Benutzer besitzt drei verschiedene Kreditkarten (Visa, AmeX, Mastercard), ein Bankkonto (Bankaccount), weiterhin ist seine Adresse kodiert (Address) und eine Versicherungsnummer (Social Insurance Number).

Die einzelnen Erweiterung werden durch sogenannte "Object Identifier" (OID) identifiziert. Diese ist eindeutig, was bedeutet, dass beispielsweise alle Felder, in denen eine Kreditkartennummer von einem speziellen Kreditkarteninstitut (beispielsweise Visa) immer dieselbe Object ID hat. Im gezeigten Beispiel der Figur 2b ist diese OID, diese sogenannte Nummer 1.3.6.1.4.15601.1. Die Definition dieser Object Identifier OID befindet sich in der ITU-T Recommendation X.660. Die OID kann entweder in einer Baumstruktur abgelegt sein, das bedeutet, alle Extensions haben denselben Elternknoten. Dieser Fall ist in der Figur 2b dargestellt. Es ist aber auch möglich, dass die Erweiterungen firmenabhängig sind. Das bedeutet, dass die Erweiterungen an verschiedenen Punktes des Baumes eingehängt werden.

Auch in der Figur 9 findet sich eine Repräsentierung des X.509 Zertifikats in Baumstruktur. Weiterhin ist in der Figur 9 zu entnehmen, dass diese Erweiterung nicht bloß als eine Bezeichnung und einem Wert bestehen kann, sondern durch weitere Informationen ergänzt werden kann. Im beschriebenen Fall der Figur 9 existiert ein weiteres Feld (Crit.), was symbolisch den Wert "true" oder "false" einnehmen kann. Wird der Wert auf true (wahr) gesetzt, so bedeutet dies, dass die Erweiterung als kritisch zu interpretieren ist. Eine mögliche Reaktion auf diesen Kritischwert kann sein, dass die Anwendung, die das Zertifikat erhält und diese Erweiterung nicht versteht, das Zertifikat als ungültig zurückweisen muss. In dem Fall, dass das Flag von kritisch auf false gesetzt ist,

kann die Anwendung das Zertifikat trotzdem verwenden, auch wenn es diese Extension nicht versteht.

Die Zertifikate können auf verschiedene Weise gespeichert werden. Standard Verfahren ist, diese zentral im Netz in einem Directory abzulegen.
Vorteilhafterweise kann der Eigentümer des Zertifikats dieses aber auch auf einem geeigneten Speichermedium mit sich tragen. Eine bekannte Methode zur Speicherung von solchen Informationen sind sogenannte "Smart Cards". Diese Smart Cards sind dem Fachmann bereits bekannt. Vorteil bei der Verwendung einer Smart Card ist, dass der Zugriff auf den Speicher, in dem das Zertifikat(eigentlich der private Schlüssel) abgelegt ist, zusätzlich durch eine PIN oder entsprechendem Paßwort geschützt werden kann. Im Falle mehrfacher falscher PIN-Eingabe wird dann der Zugang zum Speicher der Karte blockiert.
Andere Speichermedien sind jedoch vorstellbar.
In der Figur 8 findet sich eine Darstellung der Infineon Sicript Secure Token Plattform. Diese Plattform bietet zwei Stufen an Speicherzugang an. Der Userlevel ist mit einer sogenannten "User PIN" geschützt und der zweite Level mit einer weiteren "Administrator PIN". Diese "Administrator PIN" kann verwendet werden, um nach mehrfachem falschen Eingeben der "User PIN" die Karte wieder zu entsperren.

Das Speichern des Zertifikats auf einer Smart Card hat diese Vorteile:

- Sicherheit:
  Das X.509 Zertifikat und der zugehörige private Schlüssel werden in zwei verschiedenen sogenannten "Elementary Files" (EF) abgespeichert, siehe Figur 8. Der schreibende Zugriff zu der entsprechenden Datei DF_{CSP} ist mit einem Zugangscode geschützt. Das Elementary File $EF_{KeyPair}$ ist genauso geschützt. Jede Anwendung oder jeder Dienst, der den Zugriff zu dem privaten Schlüssel benötigt, muss genau diesen Zugangscode vom Benutzer erhalten. Dahingegen kann

die Ablage des $EF_{Certificate}$ immer gelesen werden, ist also nicht geschützt. Das Zertifikat in das System zu propagieren bedeutet in diesem Fall also lediglich das Kopieren des Zertifikats zu dem System.

- Mobilität:
  Smart Cards sind tragbare Speichermedien und wegen ihrer Größe kann der Benutzer sie beispielsweise in seiner Brieftasche mit sich tragen. Weiterhin kann er sie an seinem PC mit einem entsprechenden Lesergerät verwenden, genauso an öffentlichen Terminals (beispielsweise in einem Internetcafe). Der Benutzer braucht dabei nicht zu befürchten, dass der private Schlüssel kopiert wird oder im System verbleibt. Auch wenn der Benutzer seine Smart Card verliert, kann auf diese ohne den Zugangscode (PIN) nicht zugegriffen werden.

- Kompaktheit:
  Durch das erfindungsgemäße Abspeichern der verschiedenen Zahlungsmöglichkeiten (beispielsweise alle Kreditkartennummern und alle Kontonummern) auf einer Karte, ist diese besonders kompakt. Ein derartiges Abspeichern in einer Datenstruktur ist dem Fachmann bislang nicht bekannt. Weiterhin können weitere Informationen (zum Beispiel die Adresse usw.) integriert werden und machen das Userprofil damit noch kompakter.

Im Folgenden wird nun die Durchführung eines Zahlungsvorgangs mit dem X.509 Zertifikat beschrieben. In den Figuren 3a bis 3h sind verschiedene Möglichkeiten der einzelnen Nachrichten abgebildet, die vom Nutzer, dem Verkäufer oder der Bank im Verlauf des Zahlungsvorgangs benutzt werden können.
Die Übermittlung dieser Nachrichten erfolgt beispielsweise über das Internet, andere Mobilfunk- oder Festnetze sind vorstellbar.

Voraussetzung des Verfahrens ist, dass bereits durch den Nutzer eine Auswahl des Produkts erfolgt ist, sowie der Preis für dieses Produkt verhandelt wurde. Die Nachrichteneinheiten werden auf Application Level beschrieben, das bedeutet, es sind keine Bytestrukturen angegeben. Weiterhin sind die Teilnehmer des Verfahrens "online", also dauerhaft mit dem Netz verbunden.

In einem beispielhaften ersten Ablauf sind der Kunde (Consumer), der Verkäufer (Merchant) und die Bank über ein Netz, beispielsweise das Internet, verbunden. Dies soll aber keine Einschränkung für das Verfahren darstellen, andere Verbindungsmöglichkeiten sind denkbar. Die Schritte 1 bis 10 der Figur 6 werden in sequentieller Folge durchlaufen. Dabei wird angenommen, dass der Austausch des X.509 Zertifikats zwischen dem Verkäufer (Merchant) und der Bank bereits geschehen ist.

1. Der Kunde fordert vom Merchant (Verkäufer) den öffentlichen Schlüssel an, sofern er ihn noch nicht hat (Request Cert.).

2. Der Verkäufer sendete sein Zertifikat (Send. Cert.) an den Kunden.

3. Der Kunde validiert das Zertifikat. Dabei überprüft er beispielsweise, ob die Zeitgültigkeit noch nicht abgelaufen ist, und ob das Zertifikat von einer vertrauenswürdigen Autorität ausgestellt wurde. Dann sendet der Kunde seine Kaufanforderung an den Verkäufer (Purchase Order). Die Kaufanforderung kann das Format haben, wie es in Figur 3a dargestellt ist. In diesem Fall sind die Angaben der zu kaufenden Waren verschlüsselt mit dem öffentlichen Schlüssel des Verkäufers ($E(Merchant_{publickey}, goods)$, dagegen ist das X.509 Zertifikat nicht verschlüsselt. Das Versenden des X.509 Zertifikats in dieser Nachricht ist optional. Im anderen Fall holt sich der Verkäufer dieses Zertifikat aus einem öffentlichen Verzeichnis. Das Zertifikat ist nur in

dem Teil verschlüsselt, der die Kreditkarteninformation, wie vorher beschrieben, enthält.

4. Der Verkäufer entschlüsselt diese Nachricht mit seinem privaten Schlüssel. Er prüft auch hier die Gültigkeit des Zertifikats auf folgende Bedingungen:
   - Ist das Zertifikat von einer vertrauenswürdigen Autorität ausgestellt,
   - Ist die Lebensdauer des Zertifikats überschritten, und
   - Ist das Zertifikat nicht in der CRL (Certificate Revocation List).

   Erfüllt das Zertifikat eines der oben genannten Kriterien nicht, so markiert der Verkäufer es als ungültig und beendete die Sitzung mit dem Kunden.
   Anderenfalls, also wenn das Zertifikat gültig ist, sendet der Verkäufer das Zertifikat des Kunden an die Bank oder an den Kreditkartenausgeber (Verify Account), um die im Zertifikat angegebene Kreditkartennummer zu verifizieren. Diese Kreditkartennummer ist, wie bereits beschrieben, in der privaten Erweiterung des X.509 Zertifikats gespeichert, und dort nur verschlüsselt zu entnehmen.

5. Die Bank überprüft das vom Kunden empfangene X.509 Zertifikat. Die Überprüfung beinhaltet:
   - Kommt das Zertifikat von einer vertrauenswürdigen Zertifikatsautorität,
   - ist das Zertifikat abgelaufen,
   - ist das Zertifikat in der CRL (Certificate Revocation List) und
   - hat das Zertifikat die Erweiterungen, die die Informationen über Kreditkartennummern oder Kontonummern enthalten.

Ist das Zertifikat als gültig erkannt, so überprüft die Bank nun den in der Erweiterung spezifizierten Account. Ist das Konto gesperrt oder überzogen, dann sendet die Bank eine negative Antwort an den Verkäufer. Es ist vorstellbar, dass ein

vordefinierter Set an Antwortcodes zu jedem möglichen Status des Kundenkontos definiert wird, um diesen Kundenstatus zu propagieren.

Ist jedoch das X.509 Zertifikat auch in diesem zweiten Check positiv überprüft, das heisst, das Konto existiert und ist belastbar, so sendet die Bank einen speziellen Code, auch als Transaktionsnummer (TAN) bekannt, an den Verkäufer zurück (Transaction Number). Diese TAN ist in der Regel eine zufällige Zahl, die eindeutig diese Transaktion identifizieren soll.

Diese Transaktionsnummer kann auch noch mit zwei Flags bewährt werden, einen „Angefordert" und einen „Benutzt" Flag. Wenn die Transaktionsnummer zu dem Verkäufer gesendet wird, dann wird der Zustand auf "Angefordert" gesetzt. So kann die Bank Fälschungsversuche durch Kopieren dieser Transaktionsnummer verhindern. Die Bank verschlüsselt die Transaktionsnummer mit dem öffentlichen Schlüssel des Verkäufers und sendet es an den Verkäufer zurück.

6. Der Verkäufer evaluiert die Antwort der Bank und entschlüsselt diese mit seinem privaten Schlüssel.
   Ist die Antwort negativ, so beendet der Verkäufer die Sitzung mit dem Kunden.
   Im anderen Fall, wenn die Antwort positiv ist, so muss eine Transaktionsnummer von der Bank enthalten sein. Der Verkäufer formatiert die Antwort auf die Kaufanfrage des Kunden, diese Antwort ist beispielhaft in der Figur 3b dargestellt. Enthalten ist hier die Kaufsumme (Amount), der Name des Kunden (Client Name), die verschlüsselte Kontonummer, welche aus dem X.509 Zertifikat entnommen wurde (Account Encrypted), dann die angeforderten Waren (Goods) und die von Bank gelieferte Transaktionsnummer (TN). Die Zeit (Time) entspricht der Zeit am Server des Verkäufers und Name (Name) entspricht dem offiziellen Namen des Verkäufers, so wie es auch in üblichen Kreditkartentransaktionen verwendet wird. Der Kundenname und das Kundenkonto wird vom Zertifikat des Kunden entnommen. Um eine erhöhte

Privacy zu garantieren, können auch die eingefügten Waren verschlüsselt sein, hier dargestellt durch eine Hash-Funktion. Der komplette Datensatz wird dann mit dem öffentlichen Schlüssel des Kunden verschlüsselt und zum Kunden geschickt (Request Sign Order). Vorteilhafterweise speichert der Verkäufer diese Anforderung, insbesondere die Adresse und die Waren (Goods), für einen späteren Versendungsprozess.

7. Der Kunde empfängt die Nachricht vom Verkäufer und signiert diese digital (Dig. Signature). Dieses ist zu erkennen in der Figur 3c. Für die Signierung verwendet er seinen privaten Schlüssel. Wahlweise kann er mit Hilfe der Hash-Funktion seine Waren überprüfen.
Die digitale Signatur spielt hierbei eine doppelte Rolle: Zum Einen stellt es sicher, dass die Daten währen der Übertragung nicht geändert worden sind und zum Anderen seitens der angeschriebene Kunde dem Kunden entspricht, der die ursprüngliche Anforderung gesendet hat. Damit stellt es sicher, dass es sich tatsächlich um den Inhaber des X.509 Zertifikates handelt. Der Kunde verschlüsselt nun die komplette Nachricht mit dem öffentlichen Schlüssel des Verkäufers und sendet es an den Verkäufer zurück (Sign Order).

8. Der Verkäufer empfängt die verschlüsselte Nachricht und entschlüsselt sie mit seinem privaten Schlüssel. Dann verschlüsselt er sie mit dem öffentlichen Schlüssel der Bank oder des Kreditkarteninstitutes. In diesem Schritt handelt der Verkäufer nur in einer Routerfunktion (Verify Sign Order). Das Format der Nachricht entspricht demselben wie in Schritt 7, siehe Figur 3c.

9. Die Bank entschlüsselt die vom Verkäufer empfangene Nachricht mit seinem privaten Schlüssel. Danach wird die Signatur der Kundenanfrage verifiziert. Die Transaktionsnummer, die in der Nachricht vorhanden sein muss, muss auf

"Angefordert" gesetzt sein, wie vorher geschrieben. Anderenfalls ist dies ein Hinweis, dass der Verkäufer versucht hat, die Nachricht zu duplizieren. Nach Empfang der Transaktionsnummer setzt die Bank das zweite Flag für die Transaktionsnummer in seiner Datenbank auf "Benutzt". Die Bank generiert nun einen Autorisierungscode und formatiert die Daten wie in der Figur 3d angezeigt. Zeit (Time) und Bankname entsprechen dem in Schritt 6 beschriebenem. Sicherheitshalber kann die Bank nun diese Nachricht digital unterschreiben mit ihrem Autorisierungscode. Die komplette Nachricht wird danach verschlüsselt mit Hilfe des öffentlichen Schlüssels des Verkäufers und an den Verkäufer gesendet (Auth. Code).

10. Sofern der Autorisierungscode der empfangenen Nachricht positiv ist, versendet der Verkäufer seine Waren oder macht den angeforderten Dienst für den Käufer verfügbar. Weiterhin zieht er den angeforderten Geldbetrag nun vom Kreditkarteninstitut oder der Bank ein. Dann informiert der Verkäufer den Kunden, dass die Transaktion erfolgreich durchgeführt wurde (Notification). Diese Nachricht wird wieder mit dem öffentlichen Schlüssel des Kunden verschlüsselt.

Der im Vergangenem beschriebene Transaktionsprozess kann aber auch in der Anzahl der Schritte reduziert werden (siehe hierfür die Figur 5). Voraussetzung ist in diesem Fall, dass zwischen jeweils zwei Teilnehmern, dem Kunden und dem Verkäufer, und dem Verkäufer und der Bank, eine sichere Kommunikation, beispielsweise über SSL etabliert ist. Weiterhin wird angenommen, dass eine gegenseitige Authentisierung, basierend auf den X.509 Zertifikaten, zwischen den jeweiligen Teilnehmern bereits geschehen ist.

Die Schritte 1 bis 8 werden sequentiell ausgeführt. Das Format der Datenpakete ist dasselbe wie in dem vorangegangenen Beispiel der Figur 6 beschrieben. In diesem Fall besteht kei-

ne Erfordernis für eine Verschlüsselung, da die Verschlüsselung durch die SSL-Verbindung bereits gewährleistet ist. Deshalb spart man in diesem Prozess zwei Schritte ein. Im Prinzip sind die ersten zwei Schritte des Prozesses in Figur 6 eingespart, so dass der Schritt 1 der Figur 5 dem Schritt 3 der Figur 6 entspricht. Der Schritt 2 der Figur 5 entspricht dem Schritt 4 der Figur 6 und so fort.

Ein Verkaufsvorgang mit einem minimalen Nachrichtenaustausch ist in der Figur 4 dargestellt. In den beiden vorangehenden Beispielen wurde der Vorgang in zwei Schritten durchgeführt, das Bestellen und im zweiten Schritt die Signierung der Bestellung. Figur 4 zeigt nun einen Vorgang, wo beide Schritte in einem Schritt zusammengefasst werden.
Weiterhin ist in diesem Vorgehen auch keine Transaktionsnummer der Bank erforderlich. Die Transaktionsnummer wird in diesem Fall von dem Kunden selber erzeugt.

Der Nachrichtenfluss funktioniert im Folgenden:

1. Der Nutzer bereitet eine Anforderung (Sign Purchase Order) vor, er generiert sich eine Transaktionsnummer (die in diesem Fall eine wirkliche Zufallsnummer ist TN), und die gegen Kopierattacken verwendet wird. Das Format der Nachricht ist in der Figur 3e abgebildet. Das Feld "Zeit" repräsentiert die Transaktionszeit beim Kunden. Name und Kundennummer (Account) sind Werte, die aus dem Zertifikat des Kunden X.509 entnommen wurden. Die Summe (Amount) repräsentiert die Höhe der Summe dieser Kauftransaktion.
   Der Verkäufer (Merchant) ist als Name oder auch als ID, wie üblicherweise in Kreditkartentransaktionen, verwendet.
   Ein Hashwert ermöglicht es, dem Kunden seine Auflistung der georderten Waren gegenüber der Bank zu verschlüsseln, der Hash-Algorithmus ist dem Fachmann bekannt.
   Weiterhin ist in der Nachricht eine digitale Signatur (dig.sig.) enthalten, die die vorangegangenen Daten signiert. Diese Signatur versichert dem Verkäufer und der Bank, dass der Kunde die Transaktion selber initiiert hat,

und dass er der Besitzer des korrespondierenden privaten Schlüssels ist und die Transaktionsdaten während der Übertragung nicht geändert worden sind.

Das Feld "Waren" (Goods) repräsentiert die vom Käufer ausgewählten Waren, die gekauft werden sollen oder auch die Dienstleistung, dieses Feld muss für den Verkäufer lesbar sein, um im Zweifelsfall die Anforderung vervollständigen zu können.

Der Kunde hängt sein X.509 Zertifikat mit dem in den Extensions enthaltenen verschlüsselten Kreditkartennummern an die Nachricht an. Wenn diese Nachricht über das Internet verteilt wird, dann sollte der Kunde diese Nachricht zusätzlich mit dem öffentlichen Schlüssel des Verkäufers verschlüsseln.

2. Der Verkäufer überprüft das Zertifikat des Kunden auf folgende Bedingungen:
   - Ist das Zertifikat von einer vertrauenswürdigen Autorität ausgegeben,
   - ist die Lebensdauer des Zertifikats abgelaufen, und
   - ist das Zertifikat in der CRL (Certificate Revocation List).

   Wenn die Überprüfung des Zertifikats eine Fehlermeldung produziert, dann markiert der Verkäufer dieses als ungültig und beendet die Sitzung mit dem Kunden. Der Verkäufer hat außerdem die Möglichkeit, die digitale Signatur zu prüfen, beispielsweise indem er überprüft, ob der Kunde den entsprechenden privaten Schlüssel besitzt. Der Verkäufer entnimmt das Feld "Waren" (Goods) aus der enthaltenen Nachricht um sicherzustellen, dass diese Informationen nicht an die Bank gelangen, und leitet die restliche Nachricht an die Bank weiter (Verify Sign Order).

3. Die Bank überprüft das X.509 Zertifikat des Kunden auf Grund folgender Punkte:

- Ist das Zertifikat von einer vertrauenswürdigen Autorität ausgestellt,
- ist das Zertifikat abgelaufen,
- ist das Zertifikat in der CRL enthalten und
- hat das Zertifikat die privaten Erweiterungen, die die Kreditkartennummer oder Kontonummer des Kunden enthalten.

Stellt sich das Zertifikat als gültig heraus, so verifiziert die Bank die digitale Signatur um sicherzustellen, dass die Transaktion tatsächlich vom Kunden ausgelöst wurde. Danach überprüft die Bank das Konto des Kunden oder das Kreditkartenkonto, welches in dem X.509 Zertifikat enthalten war. Ist diese Kontonummer gesperrt oder ist das Konto überzogen, so sendet die Bank eine negative Antwort an den Verkäufer. Im anderen Fall, also wenn das Konto verfügbar ist, so sendet die Bank eine Antwort (Auth. Code) zurück, wie sie in der Figur 3f dargestellt ist. In diesem Fall bezeichnet das Feld "Name" den Namen der Bank oder des Kreditkarteninstituts. Die Bank signiert diese Nachricht danach mit ihrem privaten Schlüssel.

4. Im letzten Schritt macht der Verkäufer nach Erhalt des positiven Autorisierungscodes die Waren für die Käufer zugänglich oder auch die angeforderten Dienstleistungen (Notification). Weiterhin zieht er das angeforderte Geld vom Kreditkarteninstitut ein.

Das Protokoll, das in diesem Abschnitt beschrieben ist, kann beispielsweise auch über http (HyperText Transfer Protocol) oder https (HyperText Transfer Protocol Secure) ablaufen. Im Falle von http sollten die Nachrichten mit dem jeweiligen öffentlichen Schlüssel des Absenders verschlüsselt werden. Falls zwischen dem Verkäufer und der Bank ein anderes sicheres Netzwerk existiert, beispielweise ein privates Banknetz oder ein VPN (Virtual Private Network), so kann auf eine Verschlüsselung verzichtet werden.

Die Figuren 3g und 3h stellen weitere Nachrichtenformate dar, die alternativ zu den bereits beschriebenen, aus den Figuren 3a bis 3f verwendet werden können. Die Nachricht aus der Figur 3g ist beispielsweise ein anderes Format für die Nachricht aus der Figur 3c. Die Figur 3h stellt ein Nachrichtenformat entsprechend der Figur 3d dar. Dies soll deutlich machen, dass die entsprechenden Nachrichtenformate nur beispielhafter Natur sind und selbstverständlich beispielsweise durch ergänzende Felder verändert werden können.

Der Prozess, der in Figur 7 dargestellt ist, entspricht im Wesentlichen dem Vorgehen der Figur 6 mit der einzigen Ausnahme, dass die negativen Antworten (Return (False)) bei fehlgeschlagener Überprüfung von Zertifikaten mit eingefügt sind.

Eine Realisierung der erfindungsgemäßen Idee wurde bereits erprobt. Hier wurde das Windows XP als Betriebssystems verwendet, .NET Studio als Entwicklungsumgebung WES (Web Service Enhancements) als ein Extramodul für die Erzeugung von X.509 Zertifikaten. CAPICOM-Module für die Manipulation der Zertifikate, zum Beispiel, Signieren, Entschlüsseln, Verschlüsseln, Verifizieren usw. Open SSL für die Herausgabe der notwendigen Zertifikatextensions. Als Smart Card die Infineon Secrypt Smart Card und zugehörigen Tools für die Installation der Zertifikate.

Patentansprüche

1. Verfahren zur Übermittlung von ersten Informationen (Encrypted Goods) von einem Nutzer (Consumer) eines Telekommunikationsnetzes an einen ersten Anbieter (Merchant)
und von zweiten Informationen (X.509 Identity Certificate) von diesem Nutzer (Consumer) an einen zweiten Anbieter (Bank),
bei dem die ersten Informationen (Encrypted Goods) gemäß Vorgaben des ersten Anbieters (Merchant) verschlüsselt sein können und
bei dem die zweiten Informationen einen ein- oder mehrteiligen Bestandteil (Credit Card Info) enthalten, der gemäß Vorgaben des zweiten Anbieters (Bank) verschlüsselt ist und bei dem die Informationen in einer gemeinsamen Informationseinheit versendet werden.

2. Verfahren zur Übermittlung von ersten Informationen (Encrypted Goods) von einem Nutzer (Consumer) eines Telekommunikationsnetzes an einen ersten Anbieter (Merchant)
und von zweiten Informationen (X.509 Attribute Certificate) von diesem Nutzer (Consumer) an einen zweiten Anbieter (Bank),
bei dem die ersten Informationen gemäß Vorgaben des ersten Anbieters (Merchant) verschlüsselt sein können und
bei dem die zweiten Informationen einen ein- oder mehrteiligen Bestandteil (Credit Card Info) enthalten, der gemäß Vorgaben des zweiten Anbieters (Bank) verschlüsselt ist
und bei dem die zweiten Informationen von dem ersten oder zweiten Anbieter aus einem von dem ersten und zweiten Anbieter zugreifbaren Datenspeicher abgelegt sind.

3. Verfahren nach Patentanspruch 1 oder 2,
dadurch gekennzeichnet, dass
zur Ablage der zweiten Informationen eine private Erweiterung eines Zertifikates gemäß dem Standard X.509 verwendet wird.

4. Verfahren nach einem der vorigen Patentansprüche, dadurch gekennzeichnet, dass es für eine Zahlungstransaktion verwendet wird und die übertragenen ersten und/oder zweiten Informationen sich auf die Zahlungstransaktion beziehen.

5. Verfahren nach Patentanspruch 4, dadurch gekennzeichnet, dass dem Zahlungsvorgang von dem zweiten Anbieter oder von dem Nutzer eine eindeutige Transaktionsnummer (TAN) zugewiesen wird.

6. Verfahren nach Patentanspruch 4, dadurch gekennzeichnet, dass eine Identity Certificate Extension verwendet wird.

7. Verfahren nach Patentanspruch 4, dadurch gekennzeichnet, dass eine Attribute Certificate Extension verwendet wird.

8. Verfahren nach Patentanspruch 7, dadurch gekennzeichnet, dass ein Attribute Certificate genau einmal verwendet werden kann.

9. Verfahren nach einem der vorigen Patentansprüche, dadurch gekennzeichnet, dass zur Ablage des Zertifikats ein geeignetes Speichermedium, insbesondere eine Smart Card, ein Smart Dongle oder ein kontaktlos abzulesendes Speichermedium verwendet wird.

10. Verfahren nach einem der vorigen Patentansprüche, dadurch gekennzeichnet, dass das Zertifikat mit einem Passwort geschützt auf dem Speichermedium abgelegt ist.

Zusammenfassung

Verfahren zum Übermitteln von geschützten Informationen an mehrere Empfänger

Erste Informationen, die für einen ersten Empfänger bestimmt sind, werden zusammen mit zweiten Informationen, welche für einen zweiten Empfänger bestimmt sind, in einer gemeinsamen Informationseinheit an den ersten Empfänger versendet. Die ersten Informationen können dabei gemäß den Vorgaben des ersten Empfängers verschlüsselt sein. Die zweiten Informationen, welche aus mehreren Bestandteilen bestehen können, werden gemäß den Vorgaben des zweiten Empfängers verschlüsselt, beispielsweise mit einem öffentlichen Schlüssel, einem sogenannten "public key". Diese "public key" Verschlüsselungsverfahren sind bereits in verschiedenen Ausführungen und Sicherheitsstufen bekannt. Durch dieses Vorgehen wird gewährleistet, dass der erste Empfänger bei Erhalt der kompletten Information die für ihn nicht bestimmten Informationsanteile nicht entschlüsseln kann.

Figur 5

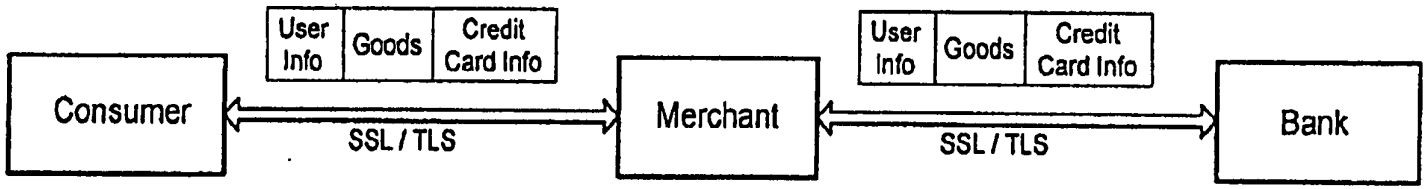
User Info
Goods
Credit Card Info
Consumer
SSL / TLS
Merchant
User Info
Goods
Credit Card Info
SSL / TLS
Bank

Fig. 1A

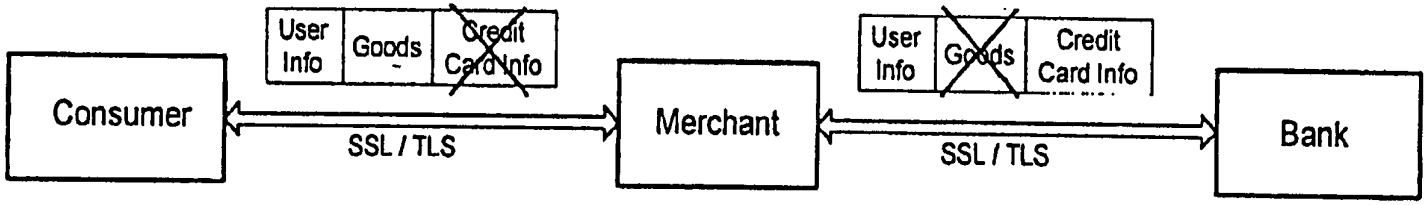
User Info
Goods
Credit Card Info
Consumer
SSL / TLS
Merchant
User Info
Goods
Credit Card Info
SSL / TLS
Bank

Fig 1B

Attribute	Encrypted attribute-Extension
VISA	$E(K_{VISAPublicKey}, CreditCardNumber)$
American Express (AMEX)	$E(K_{AMEXPublicKey}, CreditCardNumber)$
MasterCard	$E(K_{MasterCardPublicKey}, CreditCardNumber)$
Bank Account	$E(K_{BankPublicKey}, AccountNumber)$
Address	$E(K_{PostPublicKey}, Address)$
Social Insurance Number	$E(K_{InsurancePublicKey}, InsuranceNumber)$

Tabelle 1.1: New certificate extensions.

Fig. 2A

OID	Value
1.3.6.1.4.15601	Root node of new extensions
1.3.6.1.4.15601.1	Encrypted value of VISA credit card number
1.3.6.1.4.15601.2	Encrypted value of American Express credit card number
1.3.6.1.4.15601.3	Encrypted value of MasterCard credit card number
1.3.6.1.4.15601.4	Encrypted value of bank giro account number
1.3.6.1.4.15601.5	Encrypted value of address
1.3.6.1.4.15601.6	Encrypted value of insurance number

Tabelle 1.2: New private OIDs.

Fig. 2B

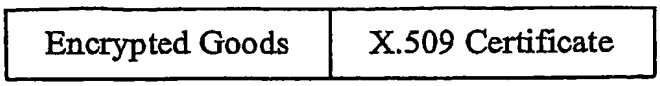

FIG 3A

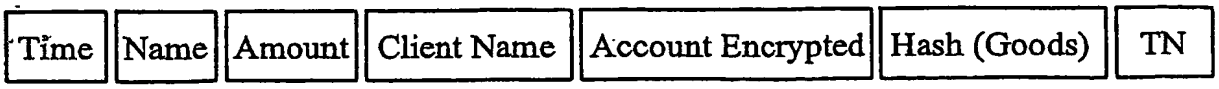

FIG 3B

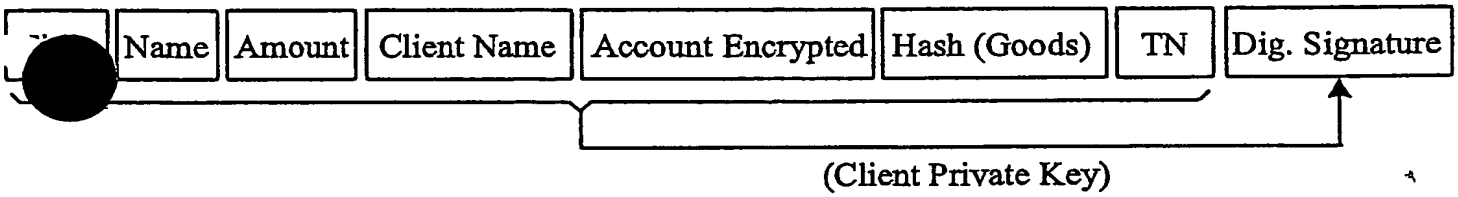

FIG 3C

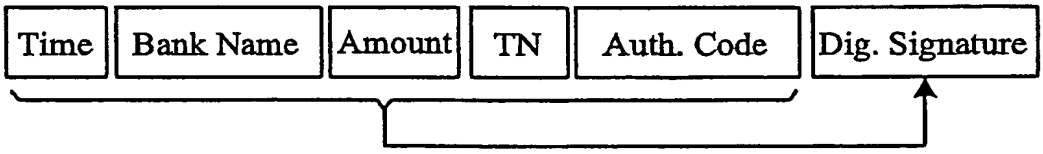

FIG 3D

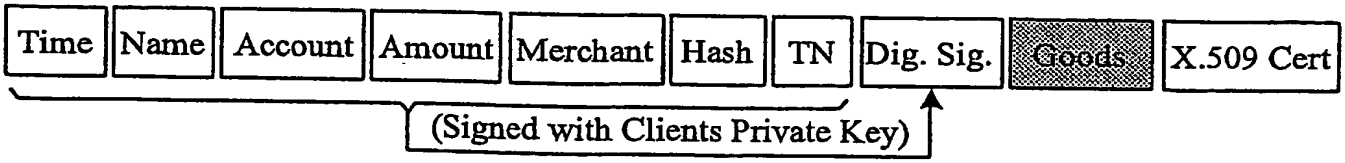

FIG 3E

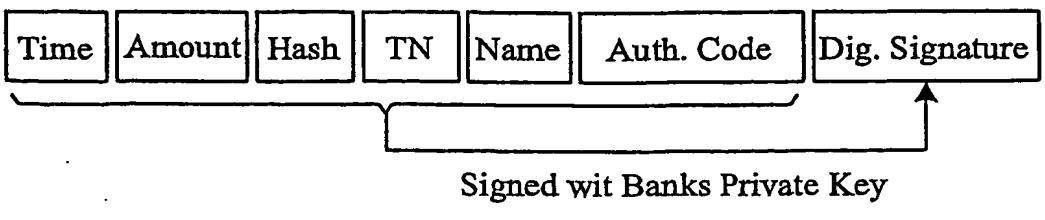

FIG 3F

User request format:

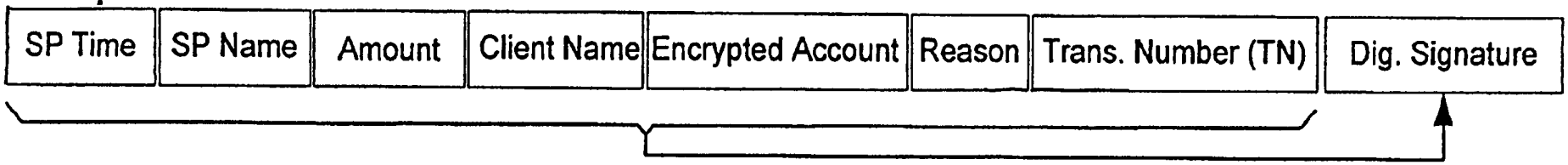

FIG 3G

Credit Card Issuer response format:

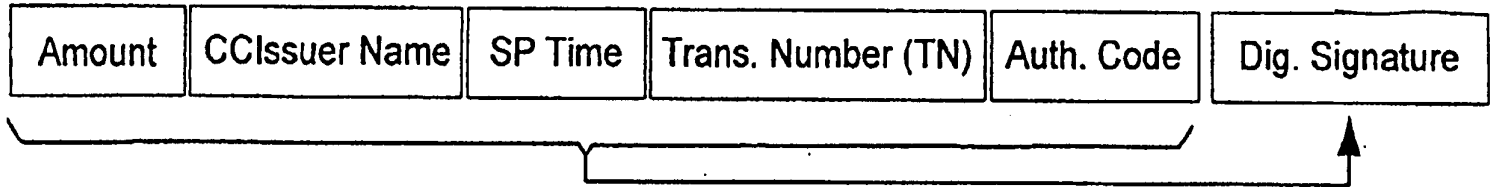

FIG 3H

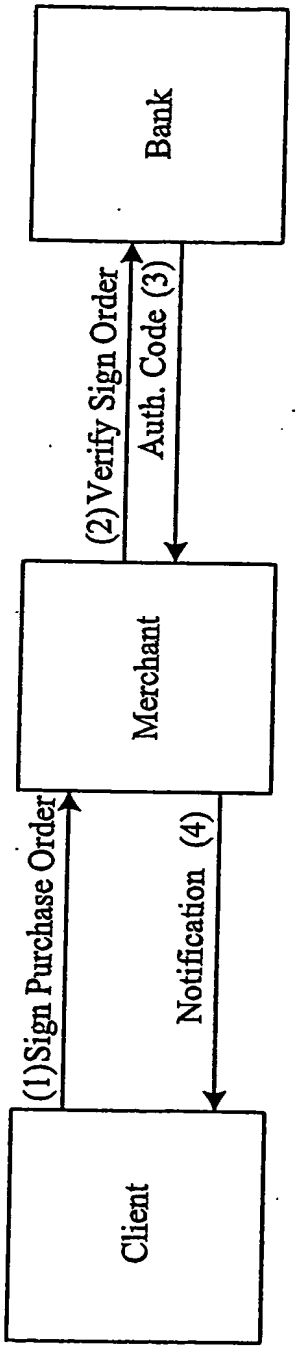
Bank
(2) Verify Sign Order
Auth. Code (3)
Merchant
(1) Sign Purchase Order
Notification (4)
Client

FIG 4

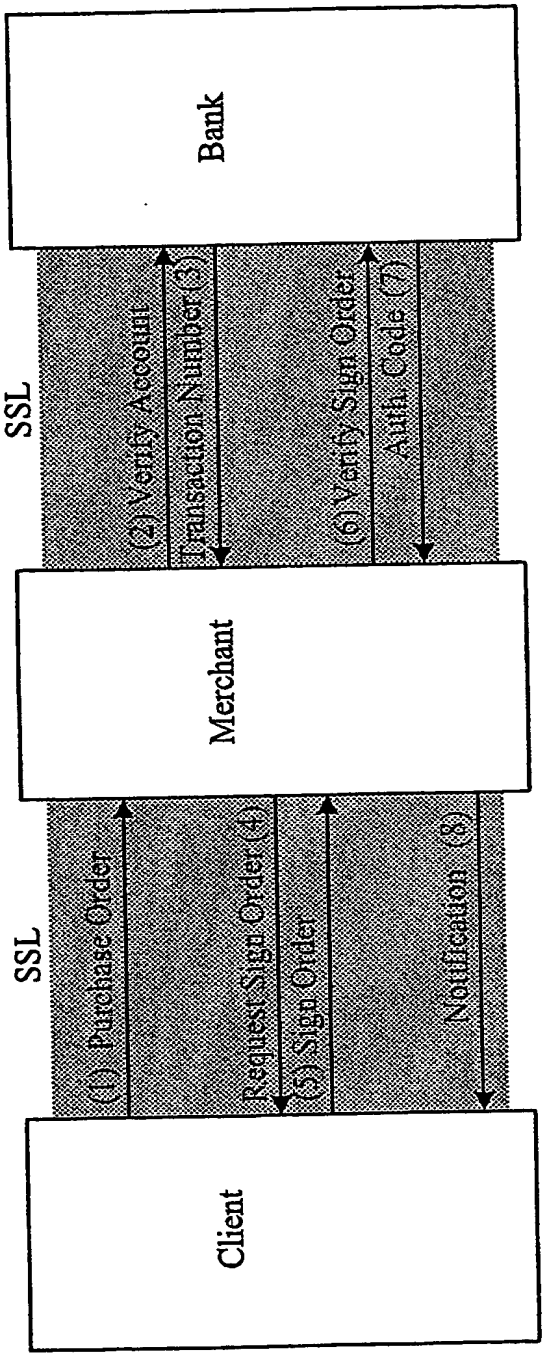
Bank
SSL
(2) Verify Account
Transaction Number (3)
(6) Verify Sign Order
Auth. Code (7)
Merchant
SSL
(1) Purchase Order
Request Sign Order (4)
(5) Sign Order
Notification (8)
Client

FIG 5

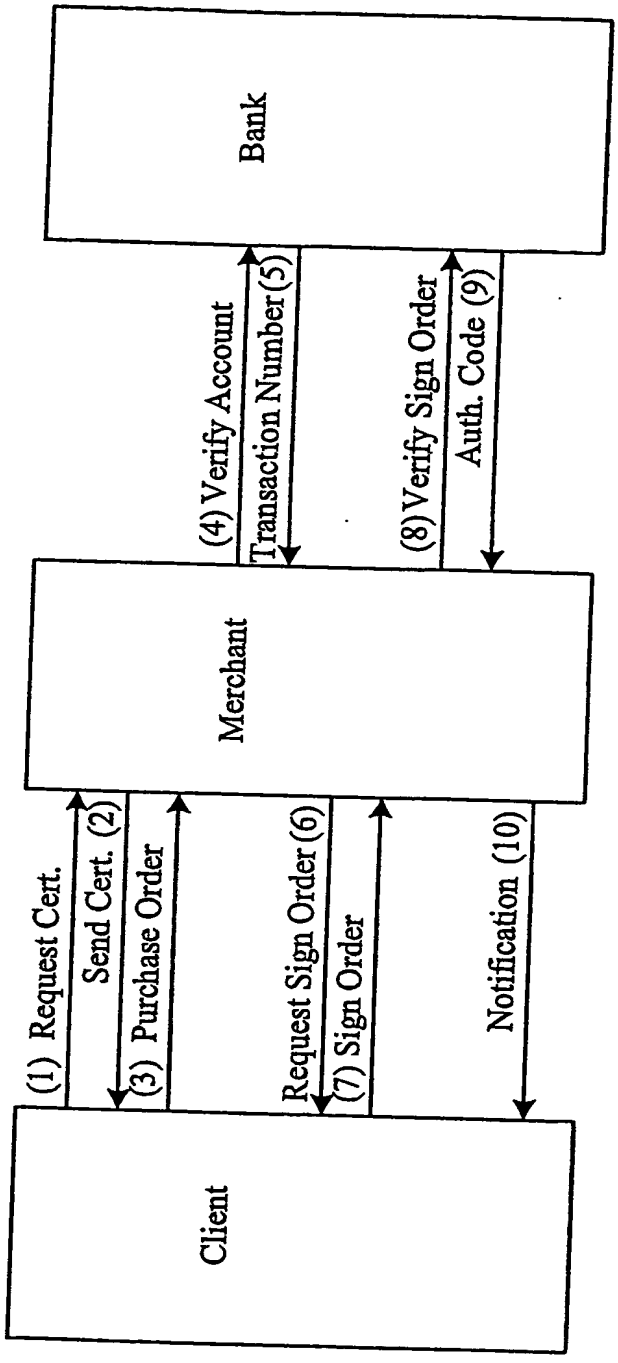
Bank
(4) Verify Account
Transaction Number (5)
(8) Verify Sign Order
Auth. Code (9)
Merchant
(1) Request Cert.
Send Cert. (2)
(3) Purchase Order
Request Sign Order (6)
(7) Sign Order
Notification (10)
Client

FIG. 6

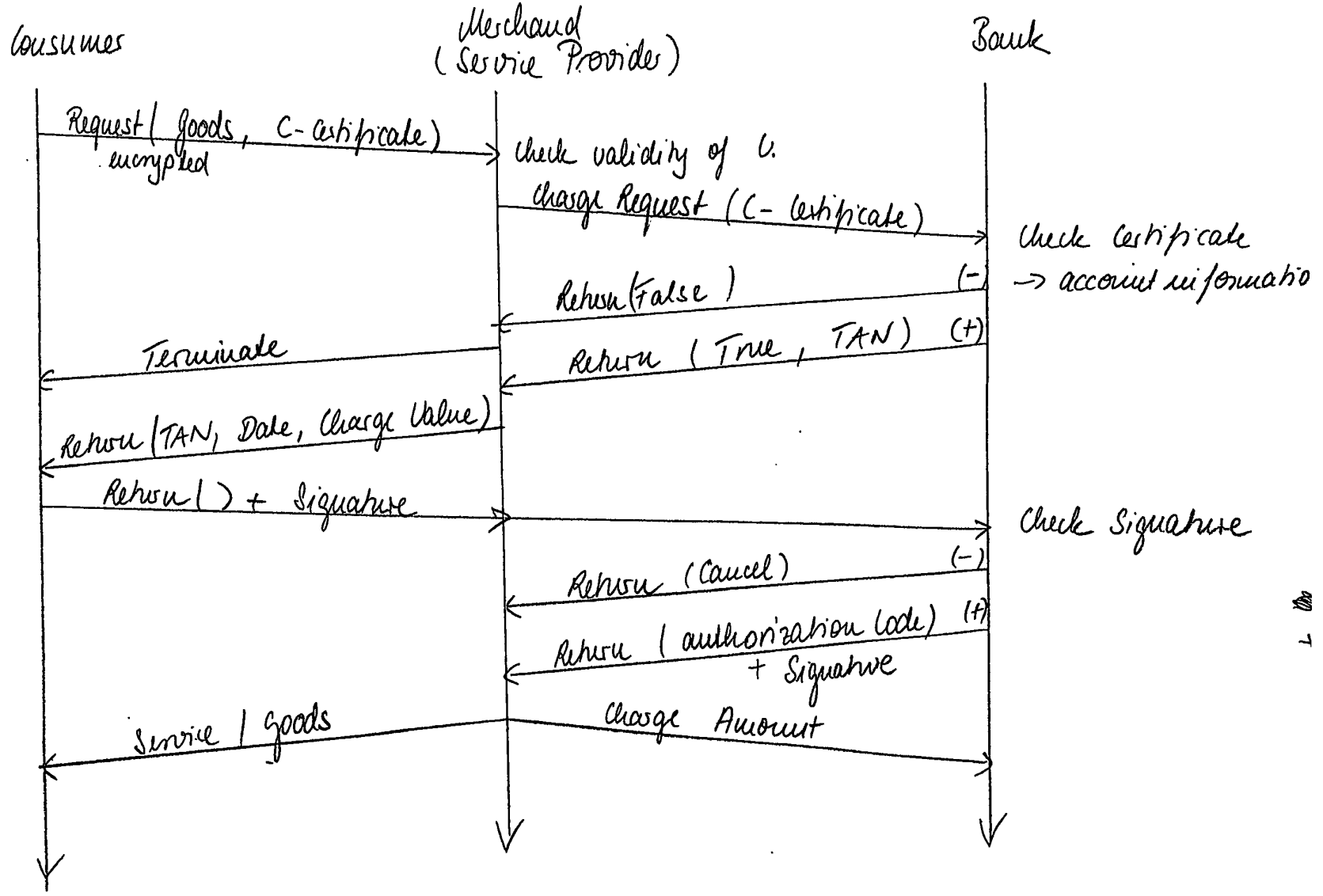
Consumer
Merchant
(Service Provider)
Bank
Request (goods, C-certificate)
encrypted
Check validity of C.
Charge Request (C-certificate)
Check certificate
→ account information
Return (False)
(-)
Terminate
Return (True, TAN)
(+)
Return (TAN, Date, Charge Value)
Return () + Signature
Check Signature
Return (Cancel)
(-)
Return (authorization code)
+ Signature
(+)
Service / goods
Charge Amount

FIG 7

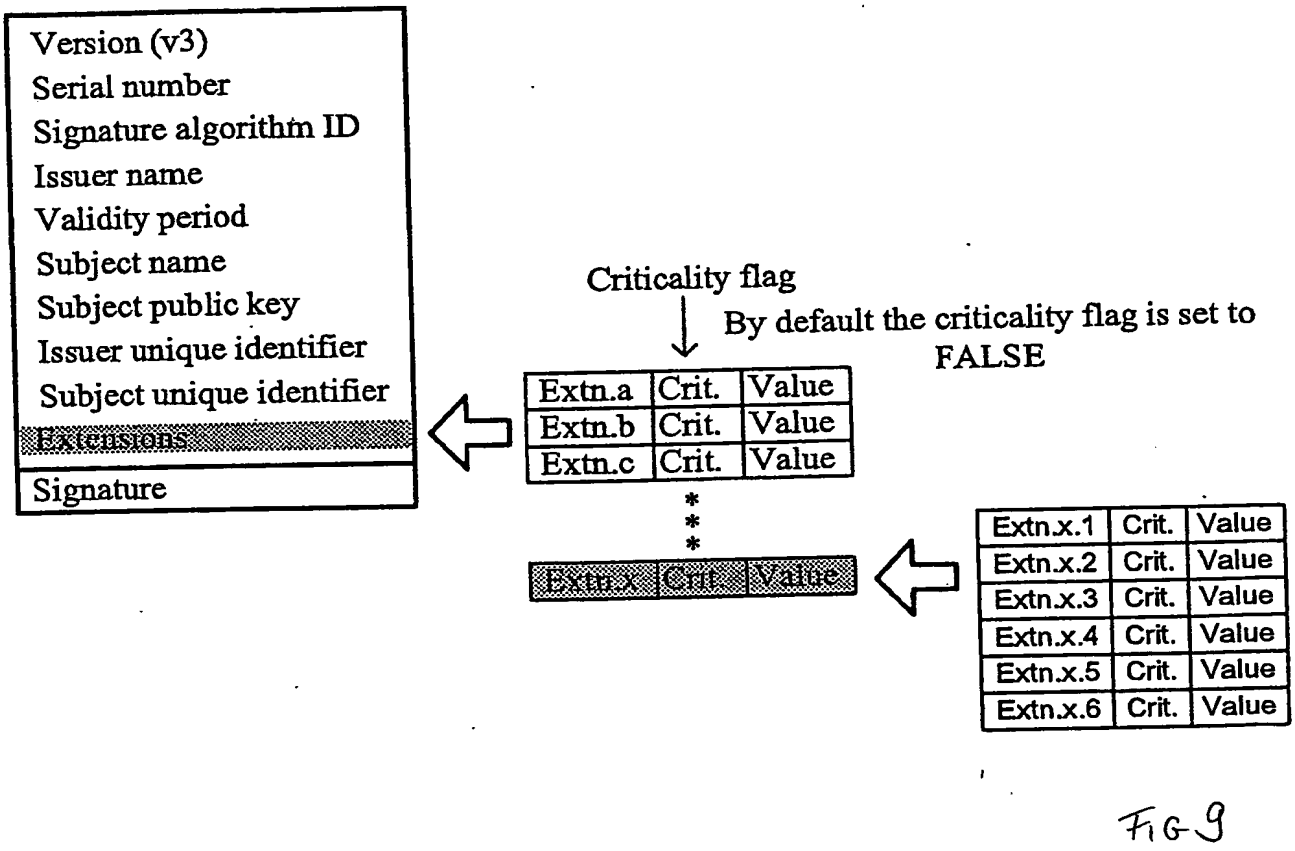
Version (v3)
Serial number
Signature algorithm ID
Issuer name
Validity period
Subject name
Subject public key
Issuer unique identifier
Subject unique identifier
Extensions
Signature
Criticality flag
By default the criticality flag is set to FALSE
Extn.a Crit. Value
Extn.b Crit. Value
Extn.c Crit. Value
Extn.x Crit. Value
Extn.x.1 Crit. Value
Extn.x.2 Crit. Value
Extn.x.3 Crit. Value
Extn.x.4 Crit. Value
Extn.x.5 Crit. Value
Extn.x.6 Crit. Value

Fig 9

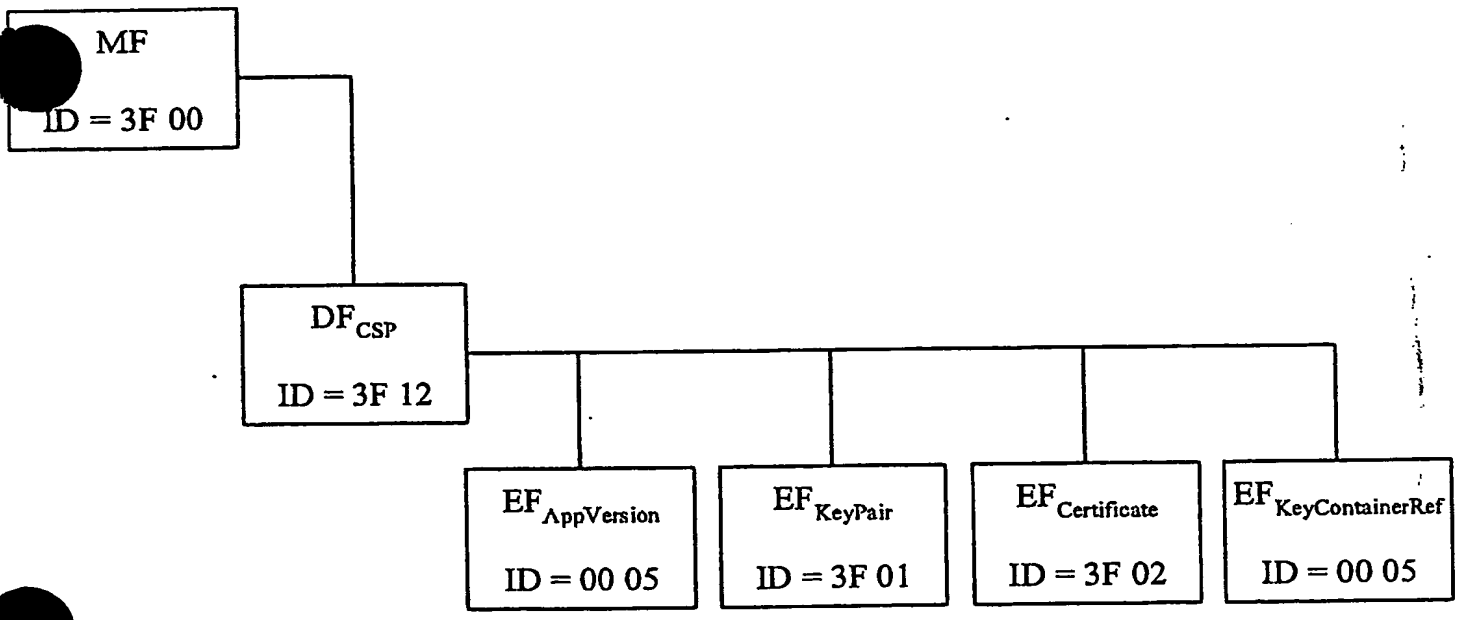
MF
ID = 3F 00
DF CSP
ID = 3F 12
EF AppVersion
ID = 00 05
EF KeyPair
ID = 3F 01
EF Certificate
ID = 3F 02
EF KeyContainerRef
ID = 00 05

FIG 8